Presented to the Court by the foreman of the Grand Jury in open Court, in the presence of the Grand Jury and FILED in the U.S. DISTRICT COURT at Seattle, Washington.

October 27 2022
Ravi Subramanian, Clerk
By _____ Deputy

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff,

v.

SERGEI POTAPENKO and
IVAN TURÕGIN,

Defendants.

NO CR22-185 RSL

INDICTMENT

The Grand Jury charges that:

INTRODUCTION

A. Defendants and Co-conspirators

1. At times relevant to this Indictment, the following individuals were involved in the conspiracies and charges set forth herein:

a. The defendant, SERGEI POTAPENKO ("POTAPENKO"), an Estonian citizen residing in Tallinn, Estonia;

b. The defendant, IVAN TURÕGIN, also known as Ivan Turygin ("TURÕGIN"), an Estonian citizen residing in Tallinn, Estonia;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

c. "Co-conspirator #1," an Estonian citizen residing in Baar, Switzerland;

d. "Co-conspirator #2," a Belarusian citizen residing in Minsk, Republic of Belarus;

e. "Co-conspirator #3," an Estonian citizen residing in Tallinn, Estonia; and

f. "Co-conspirator #4," an Estonian citizen residing in Loksa, Estonia.

B. Summary of Fraud and Money-Laundering Schemes

2. Beginning no later than about December 2013, and continuing through at least August 2022, POTAPENKO and TURÕGIN, and others, engaged in a series of interrelated fraudulent solicitations related to virtual currency. Through these solicitations, defendants induced at least hundreds of thousands of investors around the world, including in the Western District of Washington, to invest in and otherwise purchase virtual currency-related products and services based on their materially false and fraudulent pretenses, representations, and promises. POTAPENKO and TURÕGIN, and others, used the proceeds from each solicitation to fund the next solicitation; convinced victims to roll their investment interests over from one solicitation to the next; and, even more brazenly, simply kept (stole) the money victims had invested.

3. In total, through the scheme and artifice to defraud, POTAPENKO and TURÕGIN, and others, induced hundreds of thousands of victims to collectively transfer more than $550 million to accounts the defendants owned and controlled.

4. POTAPENKO and TURÕGIN, and others, using additional false and fraudulent representations, fabricated documents, and by deceit, siphoned off significant portions of the investor funds for their personal gain and benefit. More specifically, POTAPENKO and TURÕGIN, and others, funneled fraudulently-obtained victim funds through a convoluted network of shell companies, bank accounts, virtual asset service

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

providers, and virtual currency wallets, all of which they owned and controlled, directly or indirectly. They also created fraudulent documents, which they provided to financial institutions to explain their unlawful money movement, all to conceal the nature, location, source, ownership, and control of the funds.

5. POTAPENKO and TURÕGIN, and others, then used the laundered proceeds to fund an extravagant lifestyle at the expense of the victim investors.

C. Background on Virtual Currency and Mining

6. Virtual currency is a type of digital asset. Unlike traditional currency (which is sometimes called "fiat currency"), virtual currency is not issued by any government or bank. Rather, users generate and exchange virtual currency using computers operating on decentralized, peer-to-peer networks.

7. There are thousands of virtual currencies in use. Bitcoin is the most popular form of virtual currency. Other types of virtual currency can collectively be referred to as "altcoins."

8. Virtual currency mining is the process of using computers to generate new virtual currency for profit. Computers mine currency by performing operations that validate transactions and maintain the security of the virtual currency network. These verified transactions make up a decentralized, unchangeable ledger of virtual currency transactions called the "blockchain." Virtual currency miners receive newly-created currency as a reward for using their computer power to complete the operations.

9. Virtual currency mining operations require substantial computer processing power. The greater a mining operation's processing power, the more virtual currency it can be expected to produce. Processing power is measured by "hashrate," which reflects the number of calculations that the computer can perform per second.

10. "Cloud mining" or "remote mining" is an economic arrangement in which participants can, in essence, rent a specified amount of hashrate from a mining operation

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

for an agreed period of time (the contract period). During the contract period, the participant is entitled to receive a portion of the virtual currency generated by the mining operation. The participant's share of the mining proceeds is based on the amount of hashrate purchased.

11. Virtual currency holders typically use tools known as "wallets" to send, receive, and store virtual currency. Wallets vary widely in terms of their format and technological sophistication. One variety, known as "hosted" (or "custodial") wallets, are virtual currency wallets controlled by a third party—often, a company with a cloud-based, encrypted wallet platform that may be hosted on the company's servers. Users of hosted wallets may be able to access the company's platform through various digital devices, much like a traditional online banking experience. Hosted wallet providers include virtual currency exchanges, which allow their customers, for a fee, to exchange virtual currency for other virtual currencies and/or fiat currencies.

COUNT 1

(Conspiracy to Commit Wire Fraud)

12. The allegations set forth in Paragraphs 1 through 11 of this Indictment are re-alleged and incorporated as if fully set forth herein.

A. Offense

13. Beginning in or around December 2013, and continuing through at least August 2019, in King County, within the Western District of Washington, and elsewhere, the defendants, SERGEI POTAPENKO and IVAN TURÕGIN, and others known and unknown to the Grand Jury, did knowingly and willfully combine, conspire, confederate, and agree together to commit an offense against the United States, to wit: to knowingly and willfully devise and execute, and attempt to execute, a scheme and artifice to defraud, and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises; and in executing and attempting to

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

execute this scheme and artifice, to knowingly cause to be transmitted in interstate and foreign commerce, by means of wire communication, certain signs, signals and sounds, as further described below, in violation of Title 18, United States Code, Section 1343.

B. Object of the Conspiracy

14. The object of the conspiracy was for the defendants to unjustly enrich themselves and their associates by, among other things: (a) inducing participants to purchase and invest in virtual currency-related products, services, and ventures through materially false and fraudulent pretenses, representations, and promises as to the use and purpose of investment funds, the technical capabilities of the virtual currency venture, and the performance and returns of the investments; (b) diverting investor funds to virtual currency wallets and financial accounts under their custody and control; (c) utilizing investor funds for personal gain and benefit; and (d) concealing the misappropriation of investor funds through fraud and deception.

C. Manner and Means of the Conspiracy

15. The manner and means used to accomplish the conspiracy included, but are not limited to, the following:

1. HashCoins

a. Beginning no later than December 2013, POTAPENKO and TURÕGIN , and others, began operating HashCoins OÜ ("HashCoins") in Estonia. HashCoins purported to manufacture and sell virtual currency mining hardware and equipment to customers worldwide.

b. HashCoins advertised the sale of equipment capable of mining different types of virtual currencies including Bitcoin and various altcoins. HashCoins required customers to pay for the equipment in full at the time the customer ordered the equipment.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

c. In reality, throughout the period of its operation, HashCoins did not manufacture mining equipment. Instead, HashCoins sometimes purchased, assembled, and resold components manufactured by other companies. Further, HashCoins had minimal mining equipment inventory in stock and had minimal access to additional inventory. As a result, and as POTAPENKO and TURÕGIN knew, HashCoins lacked the capacity to deliver the equipment to customers on the scale, and according to the timeline, promised to customers.

d. POTAPENKO and TURÕGIN, and others, misled customers about HashCoins' ability and intention to fulfill orders. For instance, in response to customer complaints, HashCoins cited a variety of reasons to postpone deliveries, such as purported delays in the hardware certification process, driver or software updates, and production and licensing delays. Defendants denied customers' requests for refunds. Despite knowing that HashCoins had been unable to fulfill the majority of existing orders dating back to 2014, and that HashCoins would be unable to obtain additional inventory to cover those or future orders, POTAPENKO and TURÕGIN, and others, by and through their operation of HashCoins, continued to market the sale of virtual currency mining hardware and equipment well into 2016.

e. In or around May 2015, in an effort to placate customers, and to avoid refunding customers' payments for equipment that HashCoins had failed to deliver, HashCoins informed some customers that their undelivered virtual currency mining hardware and equipment was being substituted with "remote mining" or "contract mining" services. HashCoins told customers that, instead of receiving physical machines as promised, they would receive rights under mining contracts entitling the customer to a percentage of profits from a pooled remote mining operation known as HashFlare.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

2. HashFlare

f. POTAPENKO and TURÕGIN, and others, publicly launched HashFlare (www.hashflare.io) in approximately February 2015. HashFlare purported to sell access to hashrate generated by equipment HashFlare claimed to own and operate. According to HashFlare's website:

> Our service makes cryptocurrency mining available to every user. You no longer need to buy expensive equipment and spend your time setting up miners. Just select your desired capacity and earn income!
>
> *****
>
> Cloud mining offers a unique option for mining with a low cost of entry as well as minimal risk and expense, which is opposite to traditional models of mining that involve procurement, maintenance and configuration of highly specialized software.

Further, HashFlare advertised and represented that it conducted virtual currency mining in collaboration with HashCoins, which provided technical support, development, and marketing for HashFlare.

g. The HashFlare website enabled customers to purchase virtual currency mining capacity (hashrate) for a predetermined price. Customers paid for the hashrate using credit cards, bank wires, and virtual currency transfers.

h. POTAPENKO and TURÕGIN, and others, represented that HashFlare customers would receive virtual currency generated by HashFlare's mining equipment proportionate to their allocated hashrate. Customers could access their HashFlare accounts through the website and view their balance, namely, the amount of virtual currency they had purportedly generated through mining activity. HashFlare regularly updated the balances to reflect the purportedly ongoing mining activity. Defendants represented that customers could instantly withdraw their balance, or, if they chose, reinvest the proceeds to purchase additional hashrate.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

i. HashFlare's Terms of Service stated that HashFlare "enables individuals to remotely mine Cryptocurrencies for themselves using our Mining Hardware . . .." Further, "Miners will be able to receive Cryptocurrencies on the basis of the processing power of the Cloud Machine [HashFlare's remote mining network] and the period of time for which the Cloud Machine is mining. . . Those Cryptocurrencies will be transferred to your wallet upon request, if such request is confirmed."

j. POTAPENKO and TURÕGIN, and others, through the entities they operated and controlled, collected more than $550 million from customers seeking to purchase virtual currency mining capacity on hashflare.io.

k. POTAPENKO and TURÕGIN, and others, operated HashFlare as a Ponzi scheme. HashFlare did not own or lease the virtual currency mining equipment necessary to service its contracts. In reality, during the course of its operation, HashFlare engaged in virtual currency mining activity at a rate estimated to be less than one percent of the hashrate sold to customers for Bitcoin mining, and less than three percent of the hashrate sold to customers for altcoin mining.

l. The virtual currency returns and balances presented on investors' accounts were wholly fraudulent because HashFlare had not produced the represented virtual currency. To conceal this fact, when investors submitted requests to withdraw their mining proceeds, defendants either resisted making payments or paid off the investors using virtual currency defendants had simply purchased on the open market, as opposed to currency generated by genuine mining operations.

m. POTAPENKO and TURÕGIN, and others, acquired pre-existing corporate entities from a third-party vendor engaged in the sale of shell companies and used these shell companies as fronts to provide the appearance of legitimacy and to deceive customers, vendors, and financial institutions regarding the true nature of HashFlare's operations and the use of victim funds.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

n. POTAPENKO and TURÕGIN, and others, opened accounts at financial institutions and virtual asset service providers located in many countries, often in the names of shell companies and other individuals, known and unknown, working with them. POTAPENKO and TURÕGIN, and others, transferred large amounts of victim funds to and through these accounts, which they controlled, to facilitate the fraud, such as to purchase virtual currency used to pay back investors, to finance related ventures, and to funnel funds to themselves and their associates for personal gain and benefit.

o. To make the fund transfers appear legitimate and lawful, POTAPENKO and TURÕGIN, and others, submitted false information and fabricated documents, including fake invoices and contracts, related to their business ventures. For instance, POTAPENKO and TURÕGIN, and others, falsely represented to multiple banks that shell companies, which they controlled and operated, provided products and services to HashFlare, thereby providing a false pretext for large incoming fund transfers into shell company bank accounts.

3. Defendants' Refusal to Return HashFlare Victim Funds

p. POTAPENKO and TURÕGIN, and others, continuously caused HashFlare to unilaterally change the terms and conditions of its services. As the amount of new and returning customers diminished over time, POTAPENKO and TURÕGIN, and others, took steps to avoid paying returns to HashFlare customers.

q. For example, HashFlare imposed both minimum and maximum withdrawal amounts, materially restricting the amounts of purported returns customers could retrieve from their HashFlare accounts. A customer with purported returns below the minimum amount was blocked from making withdrawals, while a customer with substantial purported returns could only withdraw modest amounts at a time.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

r. On July 19, 2018, HashFlare imposed a so-called Know-Your-Customer ("KYC") requirement upon customers, which mandated that users submit identification and other information before they could continue using the platform or make withdrawals. In fact, POTAPENKO and TURÕGIN, and others, used the KYC requirement as a pretext to obstruct and delay customers' abilities to make withdrawals from their accounts.

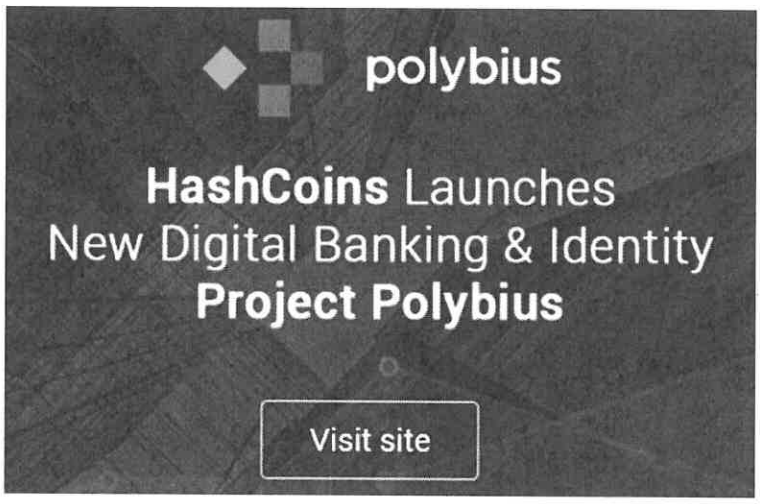
s. On July 20, 2018, HashFlare announced that it was shutting down its bitcoin mining hardware, and that it would no longer service the bitcoin mining contracts. HashFlare justified this action by claiming that, due to increased costs, bitcoin mining was no longer profitable. By refusing to service contracts, defendants deprived investors of the rights, which they had previously purchased, to earn cryptocurrency generated by ongoing mining operations. HashFlare continued to offer for sale contracts for mining of altcoins through August 2019.

t. Notwithstanding their claims that virtual currency mining had become unprofitable, the defendants diverted substantial investor funds toward the purchase and use of virtual currency mining equipment, which defendants then used for their own personal benefit.

4. Polybius

u. By no later than April 2017, leveraging what they represented to be the success of HashCoins and HashFlare, and using diverted victim funds, POTAPENKO, TURÕGIN, and others, created a new Estonian company called Polybius Foundation OÜ. POTAPENKO, TURÕGIN, and others, represented that Polybius would form a financial institution specializing in virtual currency, which would be called Polybius Bank. Defendants caused the following advertisement to be posted online:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970



v. POTAPENKO, TURÕGIN, and others, announced that Polybius Bank would be funded through an "initial coin offering" (ICO), in which investors would receive virtual tokens called Polybius tokens (symbol: PLBT). Defendants produced a prospectus stating that the PLBT tokens "represent[ed] the right to receive a part of the distributable profits" of Polybius. The prospectus represented that the proceeds of the ICO would be used to finance Polybius Bank, and that "the funds raised by the sale of the tokens will be retained by the Polybius Foundation until they will be used."

w. The defendants and their associates disseminated the Polybius prospectus to prospective investors using a HashCoins mailing list, Twitter, and the content distribution network PRNewswire, among other methods.

x. The marketing materials also advertised that the newly created bank would employ advanced technologies and offer unique services. On April 11, 2017, HashFlare sent a mass email to its customers, titled "Introducing Polybius Bank!" promoting Polybius Bank, which it called "a real revolution in the world of digital crypto-banking," directing recipients to Polybius's website (www.polybius.io), and soliciting interest in the upcoming ICO.

y. Defendants launched the ICO in or about May 2017. POTAPENKO, TURÕGIN, and others, used a virtual asset service provider based in the Western District

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

of Washington to store investment proceeds. On June 13, 2017, POTAPENKO, TURÕGIN, and others, caused an article to be published on the PRNewswire with the subheading: "Polybius cryptobank ICO has raised over $6 million in under three days, meeting the requirements to receive a European banking license."

z. Defendants raised at least $25 million from third-party investors through the ICO. Contrary to their representations that all proceeds would be retained by Polybius and used to fund Polybius Bank, defendants caused the bulk of the funds raised through the ICO to be transferred to bank accounts and virtual currency wallets controlled by POTAPENKO, TURÕGIN, and their co-conspirators.

aa. Not long after completion of the ICO in June 2017, Polybius publicly dropped any pretext that it intended to build a digital bank. POTAPENKO and TURÕGIN did not use the investment proceeds to create a digital bank as represented to investors, and to date, they have not paid the investors any dividends.

5. Use of Interstate and Foreign Wires

bb. POTAPENKO and TURÕGIN, and others, used, and caused to be used, the interstate and foreign wires in various ways in furtherance of their scheme to defraud. For example, HashFlare emailed invoices for the purchase of hashrate to victims in the Western District of Washington via interstate and foreign wire transmissions that originated outside of Washington. Similarly, investors funded their purchases of hashrate from HashFlare by means of interstate and foreign wire transmissions, including transmissions originating in the Western District of Washington and terminating outside of Washington. In addition, defendants caused the transfer of virtual currency, which was falsely represented to be the proceeds of virtual currency mining, to virtual currency wallets and through virtual asset service providers located within the Western District of Washington by means of wire transmissions originating outside of Washington. Defendants promoted the Polybius offering by sending emails that originated outside of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Washington and terminated in the Western District of Washington. Finally, defendants deposited investor proceeds from their Polybius offering to a wallet hosted by a virtual currency services provider located in the Western District of Washington. Defendants' transactions and communications with this provider caused wire transactions terminating and originating in the Western District of Washington.

All in violation of Title 18, United States Code, Section 1349.

COUNTS 2–17

(Wire Fraud)

16. The allegations set forth in Paragraphs 1 through 15 of this Indictment are re-alleged and incorporated as if fully set forth herein.

17. Beginning at a time unknown, but approximately in or about December 2013, and continuing through at least August 2019, in King County, within the Western District of Washington, and elsewhere, the defendants, SERGEI POTAPENKO and IVAN TURÕGIN, and others known and unknown to the Grand Jury, devised and intended to devise a scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises.

18. The essence of the scheme and artifice to defraud is set forth in Paragraph 14 of this Indictment and is re-alleged and incorporated as if fully set forth herein.

19. The manner and means of the scheme and artifice to defraud are set forth in Paragraph 15 of this Indictment and are re-alleged and incorporated as if fully set forth herein.

20. On or about the dates set forth below, in King County, within the Western District of Washington, and elsewhere, the defendants, and others known and unknown to the Grand Jury, having devised a scheme and artifice to defraud, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

promises, did knowingly transmit, and cause to be transmitted, the following writings, signs, signals, pictures, and sounds, for the purpose of executing such scheme, by means of wire communication in interstate and foreign commerce, each of which caused the transmission of an electronic signal between a location outside the state of Washington and within the state of Washington, and each of which constitutes a separate count of this Indictment:

Count	Date(s)	Wire Transmission
2	5/31/2017	Email from hashflare.io to Victim #1 announcing that Polybius ICO crowdfunding has started, sent from outside of Washington to Victim #1 in the Western District of Washington
3	12/12/2017	Purchase of hashrate initiated by Victim #2, within the Western District of Washington, which caused an electronic signal to be sent outside the Western District of Washington
4	12/15/2017	Email from hashflare.io attaching invoice for purchase of hashrate for virtual currency mining activity, sent from outside of Washington to Victim #2 in the Western District of Washington
5	12/15/2017	Purchase of hashrate initiated by Victim #2, within the Western District of Washington, which caused an electronic signal to be sent outside the Western District of Washington
6	12/16/2017	Purchase of hashrate initiated by Victim #3, within the Western District of Washington, which caused an electronic signal to be sent outside the Western District of Washington
7	12/17/2017	Email from hashflare.io attaching invoice for purchase of hashrate for virtual currency mining activity, sent from outside of Washington to Victim #3 in the Western District of Washington

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Count	Date(s)	Wire Transmission
8	12/21/2017	Purchase of hashrate initiated by Victim #3, within the Western District of Washington, which caused an electronic signal to be sent outside the Western District of Washington
9	12/24/2017	Transfer of Bitcoin from a virtual currency wallet, located outside the State of Washington, to a wallet controlled by Victim #3, within the Western District of Washington, represented as proceeds from virtual currency mining activity
10	2/1/2018	Transfer of Bitcoin from a virtual currency wallet, located outside the State of Washington, to a wallet controlled by Victim #3, within the Western District of Washington, represented as proceeds from virtual currency mining activity
11	2/1/2018	Transfer of Bitcoin from a virtual currency wallet, located outside the State of Washington, to a wallet controlled by Victim #4 within the Western District of Washington, represented as proceeds from virtual currency mining activity
12	4/30/2018	Email from hashflare.io attaching invoice for purchase of hashrate for virtual currency mining activity, sent from outside of Washington to Victim #2 in the Western District of Washington
13	5/1/2018	Email from hashflare.io attaching invoice for purchase of hashrate for virtual currency mining activity, sent from outside of Washington to Victim #2 in the Western District of Washington
14	5/1/2018	Purchase of hashrate initiated by Victim #2, within the Western District of Washington, which caused an electronic signal to be sent outside the Western District of Washington
15	5/3/2018	Email from hashflare.io attaching invoice for purchase of hashrate for virtual currency mining activity, sent from outside of Washington to Victim #2 in the Western District of Washington

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Count	Date(s)	Wire Transmission
16	5/3/2018	Purchase of hashrate initiated by Victim #2, within the Western District of Washington, which caused an electronic signal to be sent outside the Western District of Washington
17	5/4/2018	Purchase of hashrate initiated by Victim #2, within the Western District of Washington, which caused an electronic signal to be sent outside the Western District of Washington

21. The Grand Jury further alleges that these crimes were committed during, and in furtherance of, the offense charged in Count 1.

All in violation of Title 18, United States Code, Sections 1343 and 2.

COUNT 18

(Conspiracy to Commit Money Laundering)

22. The allegations set forth in Paragraphs 1 through 21 of this Indictment are re-alleged and incorporated as if fully set forth herein.

A. The Offense

23. Beginning at a time unknown to the Grand Jury, but no later than April 2015, and continuing through at least August 2022, within the extraterritorial jurisdiction of the United States, at King County, within the Western District of Washington, and elsewhere, the defendants, SERGEI POTAPENKO and IVAN TURÕGIN, and others known and unknown to the Grand Jury, knowingly combined, conspired, confederated, and agreed together and with each other, and with others known and unknown to the Grand Jury, to commit offenses against the United States, to wit:

a. to knowingly conduct and attempt to conduct financial transactions affecting interstate and foreign commerce, which transactions involved the proceeds of specified unlawful activity, that is, Conspiracy to Commit Wire Fraud in violation of Title 18, United States Code, Section 1349, and Wire Fraud in violation of Title 18,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

United States Code, Section 1343, knowing that the transactions were designed in whole and in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity, and knowing that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i);

b. to transmit and transfer, and attempt to transmit and transfer, monetary instruments and funds, including one or more virtual currencies, from a place in the United States, to and through a place outside the United States, and to a place in the United States from or through a place outside the United States, with the intent to promote the carrying on of specified unlawful activity, that is, Conspiracy to Commit Wire Fraud in violation of Title 18, United States Code, Section 1349, and Wire Fraud in violation of Title 18, United States Code, Section 1343, all in violation of Title 18, United States Code, Sections 1956(a)(2)(A); and

c. to knowingly engage and attempt to engage in monetary transactions by, through and to a financial institution, affecting interstate and foreign commerce, in criminally derived property of a value greater than $10,000, such property having been derived from a specified unlawful activity, that is, Conspiracy to Commit Wire Fraud in violation of Title 18, United States Code, Section 1349, and Wire Fraud in violation of Title 18, United States Code, Section 1343, in violation of Title 18, United States Code, Section 1957.

B. Object of the Conspiracy

24. The objects of the conspiracy were:

a. to conceal and disguise the nature, location, source, ownership, and control of proceeds of Conspiracy to Commit Wire Fraud in violation of Title 18, United States Code, Section 1349, and Wire Fraud in violation of Title 18, United States Code, Section 1343;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

b. to promote the carrying on of Conspiracy to Commit Wire Fraud in violation of Title 18, United States Code, Section 1349, and Wire Fraud in violation of Title 18, United States Code, Section 1343; and

c. to illegally enrich the conspirators.

B. Manner and Means of Conspiracy

25. The manner and means used to accomplish the conspiracy include, but are not limited to, the following:

a. POTAPENKO and TURÕGIN, and others, accepted HashFlare victim payments in the form of fiat and virtual currencies, which promoted the HashFlare Ponzi scheme. POTAPENKO and TURÕGIN, and others, transferred these HashFlare victim payments to accounts and wallets held outside of the United States.

b. During the conspiracy, POTAPENKO and TURÕGIN, and others, engaged in financial transactions designed to conceal the nature, location, source, ownership, and control of proceeds of the wire fraud conspiracy and direct those proceeds to accounts held for their benefit. Some of the wire fraud proceeds comprised funds in accounts holding United States dollars and virtual currency held in wallets hosted by virtual asset service providers based in the United States.

c. The defendants used shell companies, including Dalmeron Projects LP ("Dalmeron") and Ecohouse Networks LP, and then created bank accounts in the names of those shell companies. The defendants and others provided fraudulent documentation to the financial institutions with false explanations of the nature and sources of funds transferred to those bank accounts. To support POTAPENKO and TURÕGIN's false statements about Dalmeron's role, the defendants, co-conspirator #3, co-conspirator #4, and others created and sent sham and misleading documents, such as fake contracts and invoices for the services that Dalmeron supposedly performed.

d. To justify the movement of funds from one entity they controlled to another, the defendants, co-conspirator #2, co-conspirator #3, co-conspirator #4, and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

others fabricated loan agreements. They then transferred funds between accounts held at different financial institutions, providing the fake loan agreements as the reason for the transfers.

e. POTAPENKO and TURÕGIN, and others, also transferred funds between accounts holding United States dollars and accounts holding Euros in order to further conceal the nature, location, and source of victim funds.

f. POTAPENKO, TURÕGIN, co-conspirator #1, and others opened accounts at virtual asset service providers, in their own names or in the names of entities that they controlled. POTAPENKO, TURÕGIN, and others also controlled numerous unhosted wallets. POTAPENKO, TURÕGIN, and co-conspirator #1 maintained control and approval over deposits of HashFlare victim funds and Polybius ICO proceeds into various accounts, including addresses at virtual asset service providers and unhosted wallets. Some of the virtual asset service providers used by the defendants to engage in financial transactions are located in the United States, including one or more headquartered in the Western District of Washington.

g. POTAPENKO and TURÕGIN, and others, transferred large amounts of bitcoin representing HashFlare victim funds from their accounts at a virtual asset service provider using a series of transactions in which a smaller amount of bitcoin is transferred to a new address each time. In each transaction, some quantity of bitcoin "peeled off" the chain to a new address, and the remaining balance transferred to the next address in the chain. POTAPENKO and TURÕGIN used this "peel chain" technique to conceal the movement of HashFlare customer funds to bitcoin addresses that were used to repay other victims. POTAPENKO and TURÕGIN used these transactions to perpetuate their fraud by preventing victims from discovering that HashFlare lacked the represented mining operations.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

h. POTAPENKO and TURÕGIN, and others, also transferred HashFlare victim payments to an account at a virtual asset service provider they controlled and converted customer funds from one type of virtual currency to another before repaying victims with the purpose of concealing the source of the virtual currency sent to victims.

j. POTAPENKO and TURÕGIN, and others, transferred some of the remaining HashFlare victim payments to accounts and wallets they and their co-conspirators controlled, including but not limited to, unhosted wallets, an account used to make travel and clothing-related purchases, and for the purchase of virtual currency mining equipment. POTAPENKO and TURÕGIN, and others known and unknown, engaged in monetary transactions of more than $10,000 derived from victims of the HashFlare Ponzi Scheme and the Polybius ICO to and from accounts held in their names or the names of entities they owned and controlled.

All in violation of Title 18, United States Code, Section 1956(h).

FORFEITURE ALLEGATION

26. The allegations set forth in Paragraphs 1 through 25 of this Indictment are re-alleged and incorporated as if fully set forth herein.

27. Upon conviction of any of the offenses charged in Counts 1 to 17, SERGEI POTAPENKO and IVAN TURÕGIN shall each forfeit to the United States any property constituting or derived from proceeds such defendant obtained directly or directly, as a result of the offense. All such property is forfeitable pursuant to Title 18, United States Code, Section 981(a)(1)(C), by way of Title 28, United States Code, Section 2461(c). This property includes, but is not limited to, a sum of money reflecting the proceeds such defendant personally obtained from the offense.

28. Upon conviction of the offense charged in Count 18, SERGEI POTAPENKO and IVAN TURÕGIN shall each forfeit to the United States any property

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

involved in the offense. All such property is forfeitable pursuant to Title 18, United States Code, Section 982(a)(1). This property includes, but is not limited to, a sum of money reflecting the property involved in such offense.

29. **Substitute Assets.** If any of the above-described forfeitable property, as a result of any act or omission of the defendant,

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the Court;

d. has been substantially diminished in value; or,

e. has been commingled with other property which cannot be divided without difficulty,

it is the intent of the United States to seek the forfeiture of any other property of the defendant, up to the value of the above-described forfeitable property, pursuant to Title 21, United States Code, Section 853(p).

FINDINGS AS TO FORFEITURE NEXUS

30. The allegations set forth in Paragraphs 1 through 29 of this Indictment are re-alleged and incorporated as if fully set forth herein.

31. The grand jury further finds probable cause to believe that, upon conviction of the offense charged in Count 18 of this Indictment, SERGEI POTAPENKO and IVAN TURÕGIN shall each forfeit to the United States as property involved in the offense, pursuant to 18 U.S.C. § 982(a)(1):

a. the following real properties located in Estonia:

1. Tartu mnt 83, Kesklinna linnaosa, Tallinn, Harju County (Units: 103, 407, 501, 502, 503, 504, 505, 506, PK5, PK6, PK7, PK34, PK37, PK38, PK39, PK41, PK42, PK43, PK44)

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

2. Kiikri tn 2, Kesklinna linnaosa, Tallinn, Harju County (Units: 32, 42, 47, 54, 65, 66, 70, 71, 72, 76, P-58, P-59, P-61, P-62, P-77, P-78, P-79, P-80, P-81, P-82, P-89, P-90, P-96, P-97, P-98, P-99, P-100, P-101, P-104, P-105);
3. Padriku tee 9, Pirita District, Tallinn, Harju County, 3-5 (building no. 3);
4. Supluse pst 1, Pirita linnaosa, Tallinn, Harju County;
5. Padriku tee 16, Pirita District, Tallinn, Harju County, 4-11 (building no. 4);
6. Mardisalu tn 2, Peetri alevik, Rae vald, Harju County;
7. Mardisalu tn 8, Peetri alevik, Rae vald, Harju County;
8. Häälinurme tn 9, Peetri alevik, Rae vald, Harju County;
9. Lauri tee 9, Pirita District, Tallinn, Harju County;
10. Lauri tee 9a, Pirita District, Tallinn, Harju County;
11. Padriku tee 9, Pirita District, Tallinn, Harju County, 2-2 (building no. 2);
12. Kuusenõmme tee 19, Pirita District, Tallinn, Harju County;
13. Villardi tn 11-5, Kesklinna District, Tallinn, Harju County, 5;
14. Villardi tn 11-G4, Kesklinna District, Tallinn, Harju County, G4;
15. Kuusenõmme tee 17, Pirita District, Tallinn, Harju County;
16. Kuusenõmme tee T3, Pirita District, Tallinn, Harju County;
17. Kuusenõmme tee 15, Pirita District, Tallinn, Harju County;
18. Rannasalu tee 81a, Katase Village, Alutaguse Parish, Ida-Viru County;
19. Rannasalu tee 81b, Katase Village, Alutaguse Parish, Ida-Viru County;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

20. Rannasalu tee 81c, Katase Village, Alutaguse Parish, Ida-Viru County;
21. Võrgu tee, Katase Village, Alutaguse Parish, Ida-Viru County;
22. Rannasalu tee 123, Katase Village, Alutaguse Parish, Ida-Viru County;
23. Kaare, Katase Village, Alutaguse Parish, Ida-Viru County;
24. Kadaku, Katase Village, Alutaguse Parish, Ida-Viru County;
25. Rannasalu tee 83a, Katase Village, Alutaguse Parish, Ida-Viru County;
26. Käbi, Katase Village, Alutaguse Parish, Ida-Viru County;
27. Rebasesaba tee 6, Pirita District, Tallinn, Harju County, 2;
28. Järvemetsa tee 5, Peetri Small Borough, Rae Parish, Harju County;

b. the following vehicles located and registered in Estonia:

1. one 2018 Audi A7 Sportback (gray), registered to Burfa Media OÜ;
2. one 2019 BMW X7 M50D (gray), registered to Burfa Media OÜ;
3. one Lexus RX450H (dark green), registered to Felamay OÜ;
4. one 2018 Mercedes-Benz AMG G 63 (gray), registered to Ivan Turõgin;
5. one 2017 Audi SQ7s (gray), registered to Burfa Tech OÜ; and
6. one 2017 Audi SQ7s (gray), registered to Burfa Tech OÜ.

c. all funds in the following bank accounts located in Estonia:

1. AS LHV Pank account with IBAN EE947700771004802203, held in the name of Felmaway OÜ;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

2. AS LHV Pank account with IBAN EE627700771002171363, held in the name of Sergei Potapenko; and

d. the following virtual currencies and associated funds:

1. all funds—including cryptocurrencies—from a Bitcoin Suisse account associated with the bitcoin deposit address of 3Mf6LDdHGUCnFddz1CRxkBF6gWrC3RDSpR located in Switzerland;
2. all bitcoin, and any and all virtual currency derived therefrom, held by public address 3CCxFk5tDkzbbJ6qJ1j3XTchh6yBuNahFd;
3. all ether, and any and all virtual currency derived therefrom, held by public address 0xfF575a22975CC413771825EB84c163189A4d5D22;
4. all bitcoin, and any and all virtual currency derived therefrom, held by public address 38zkvJL6ZSM8tS7DFw4V37gBxqj8VVBFS9;
5. all bitcoin, and any and all virtual currency derived therefrom, held by public address 3JQZFeomJtgQvfhJPriibVVUcmDDvbCu4L;
6. all ether, and any and all virtual currency derived therefrom, held by public address 0x37Aa343C7b3A8d5cB7E1D53e262BcE5c56840DC0;
7. all ether, and any and all virtual currency derived therefrom, held by public address 0x05524556b53254ea27bF85C572Ff173A9b72e049;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

8. all bitcoin, and any and all virtual currency derived therefrom, held by public address 33oxyJj3rUyY9h9A2LMev8hGp9LfTPRFPT;
9. all bitcoin, and any and all virtual currency derived therefrom, held by public address bc1qq7t39xw5zmquvrxqpcw4xmrmj968geueufjwh9;
10. all bitcoin, and any and all virtual currency derived therefrom, held by public address bc1q3neh8n6e0e2hqp5v50498je5kjp5nv0s52j6sy;
11. all bitcoin, and any and all virtual currency derived therefrom, held by public address bc1qu7w3m03juknja5ecc8fr9zn2umcfc3rkmypwk5;
12. all ether, and any and all virtual currency derived therefrom, held by public address 0x6B0fAA0f7F52CDEa18802AeAbfA6CFD18D2B3785;
13. all ether, and any and all virtual currency derived therefrom, held by public address 0x586fe50a5D373fBa9EfcF0fdEca9C62979E855Ed;
14. all ether, and any and all virtual currency derived therefrom, held by public address 0xBB15B769E9Faf9A86186Db6a12aB72A6f56AE7d1; and
15. all bitcoin, and any and all virtual currency derived therefrom, held by public address 3M19ou5uw5CYzw34tgZnbSWMk3gsSwhNL3.

(items d.2-d.15 are believed to be located in Estonia);

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

e. the following virtual currency miners and equipment located in Estonia:

1. 135 INNO3D P106*9 miners located at Narva-2 Container, NRN02-E;
2. 135 INNO3D P106*9 miners located at Narva-2 Container, NRN02-F;
3. 352 INNO3D P106*9 miners located at Laki DC, LKI03;
4. 408 INNO3D P106*9 miners located at Narva-1, NRV01-A;
5. 408 INNO3D P106*9 miners located at Narva-1, NRV01-B;
6. 408 INNO3D P106*9 miners located at Narva-1, NRV01-C;
7. 408 INNO3D P106*9 miners located at Narva-1, NRV01-D;
8. 483 INNO3D P106*9 miners located at Narva-2, NRN02-B; and
9. 483 INNO3d P106*9 miners located at Narva-2, NRN02-C.
10. 380 INNO3D P104*7 miners located at Narva-2, NRN02-C;
11. 126 Antminer S17PRO miners located at Narva-1, NRV01-E;
12. 136 Antminer S17PRO miners located at Narva-1, NRV01-F;
13. 188 Antminer S19JPRO miners located at Narva-1, NRV01-F;
14. 198 Antminer S19JPRO miners located at Narva-1, NRV01-E; and
15. 240 Antminer S17PRO miners located at Narva-2 Container, NRN02-F.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

A TRUE BILL:

DATED: ~~10/28/2022~~ 10/27/2022 (CSJ)

Signature of Foreperson redacted pursuant to the policy of the Judicial Conference of the United States.

FOREPERSON

NICHOLAS W. BROWN
United States Attorney

BRENT S. WIBLE
Acting Chief, Money Laundering and Asset Recovery Section
Criminal Division, Department of Justice

ANDREW C. FRIEDMAN
Assistant United States Attorney

SETH WILKINSON
Assistant United States Attorney

JEHIEL I. BAER
Assistant United States Attorney

ADRIENNE E. ROSEN
Trial Attorney
Money Laundering and Asset Recovery Section
Criminal Division, Department of Justice

OLIVIA ZHU
Trial Attorney
Money Laundering and Asset Recovery Section
Criminal Division, Department of Justice

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970